

Integrating Cybersecurity with Emergency Operations Plans (EOPs) for Institutions of Higher Education (IHEs)

Amy Banks, U.S. Department of Education, Center for School
Preparedness, Office of Safe and Healthy Students

DeShelle Cleghorn, U.S. Department of Homeland Security,
Industry Engagement and Resilience Branch,
Office of Cybersecurity and Communications



Welcome & Introductions

Welcome

Housekeeping
Items

Speakers

Agenda

Background on the *Guides* and Integrating Cybersecurity into the Six Step Planning Process

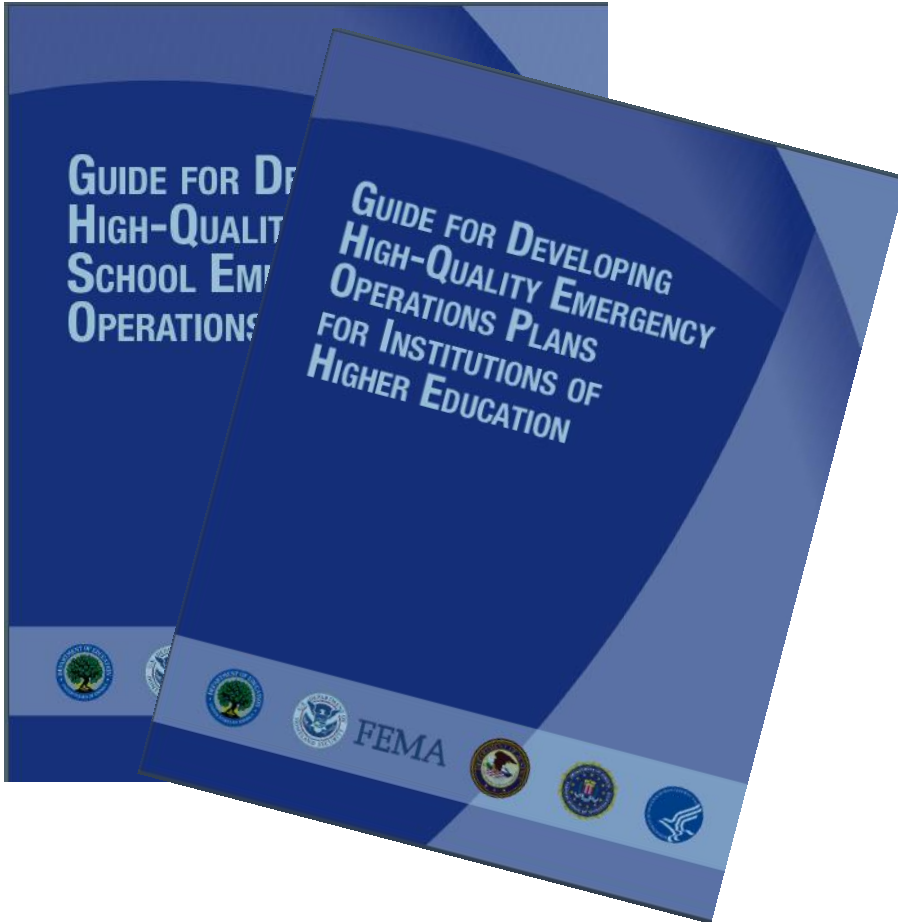
Overview of Cybersecurity

Landscape of IHE Cyber Threats and Trends

DHS Cybersecurity Resources, Programs, and Tools for IHEs

Q&A Session

The *Guide*



- ☐ Released by the Obama Administration on June 18, 2013
- ☐ Developed in collaboration with, and the first joint product of, ED, DHS, FEMA, DOJ, FBI, and HHS
- ☐ Accessible at <http://rem.s.ed.gov>

Presidential Policy Directive (PPD-8)

National Preparedness Directive

**Describes the nation's
approach to
preparedness**

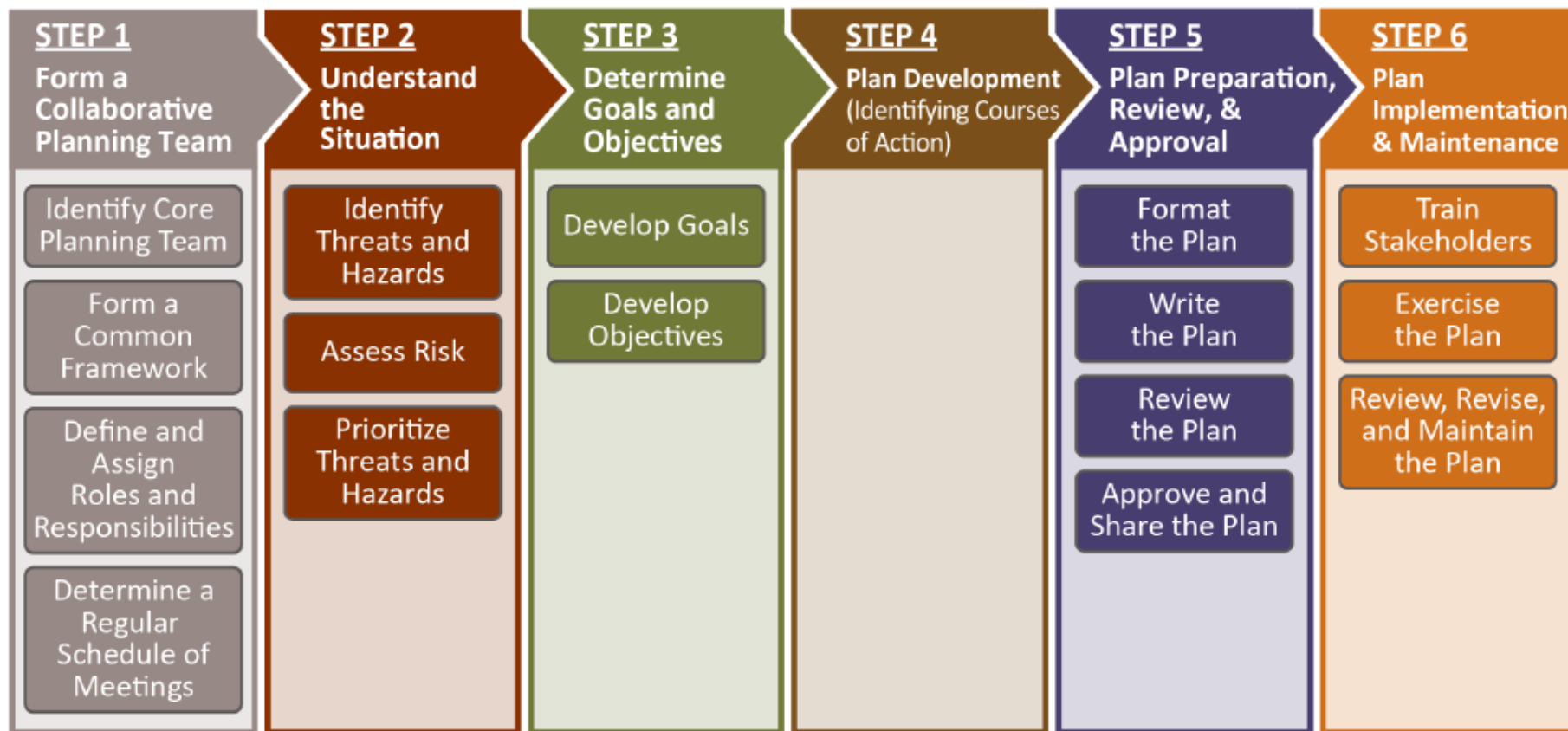
**Aims to facilitate an
integrated approach and
align planning at all
levels and with all
sectors**

Five Preparedness Missions

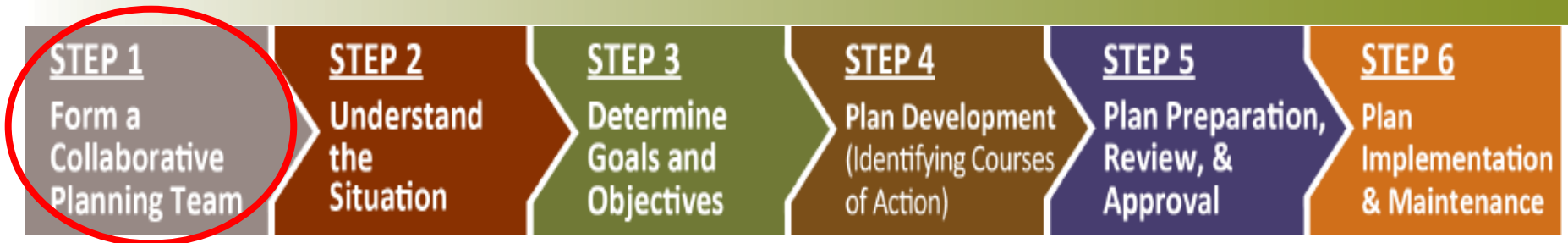


an incident or emergency

Steps in the Planning Process



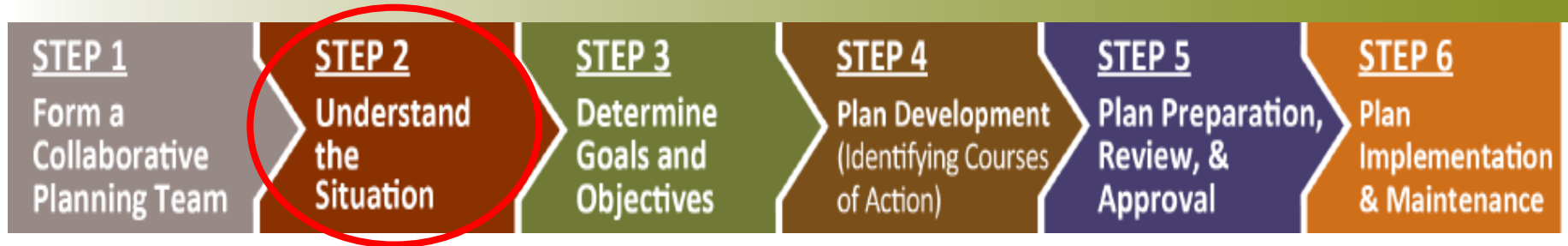
Step 1: Form a Collaborative Planning Team



Team members should include personnel who have a role in both cybersecurity and in managing a cyber incident or emergency. A collaborative planning team may include the representatives from the following areas:

- *Central Administration*
- *Academic Affairs*
- *Human Resources*
- *Business Office*
- *EMS*
- *Information Technology (IT) and Security Services*
- *Environmental Health and Safety*
- *Counseling and Mental Health*
- *Food Services*
- *Facilities and Operations*
- *U.S. Computer Emergency Readiness Team (US-CERT)*

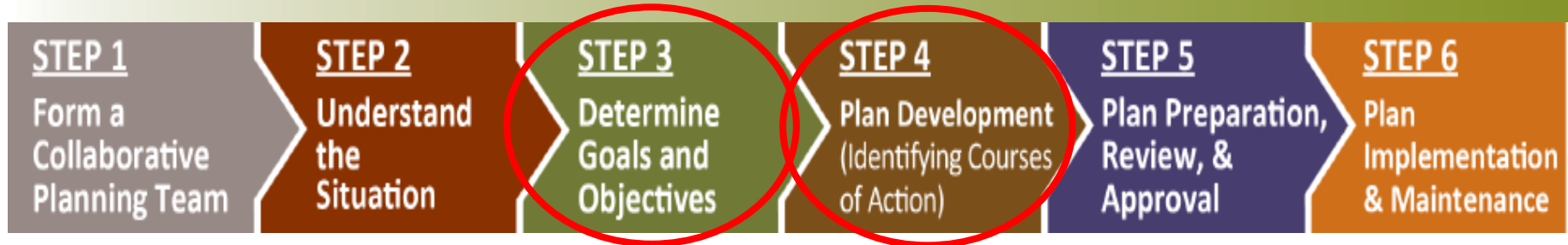
Step 2: Understand the Situation



Step 2

- Identify cyber threats and hazards.
- Assess the cyber risk.
- Identify the cyber vulnerabilities.

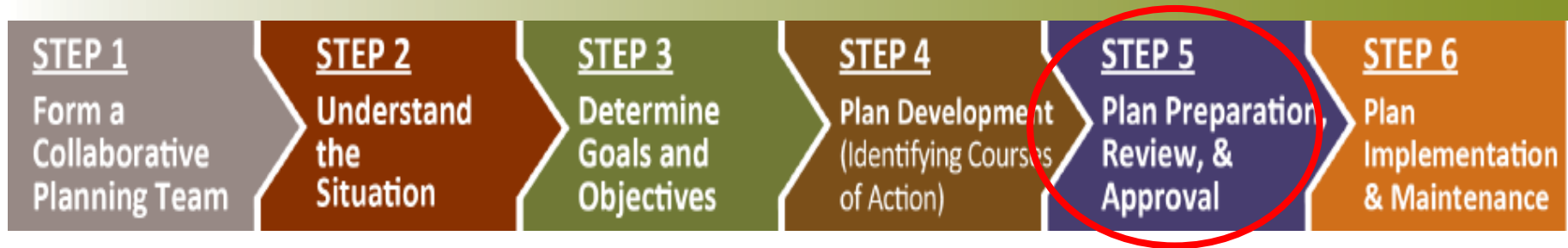
Steps 3 & 4: Develop Goals, Objectives, and Courses of Action



Steps 3 and 4

- Develop goals and objectives for each cyber threat identified in Step 2 and develop a variety of measures to prevent cyber threats.
- Common action steps to address cybersecurity may overlap with other action steps (functions) to address other emergencies.
- These steps may be categorized into a cybersecurity annex or a cyber threat- and hazard-specific annex.

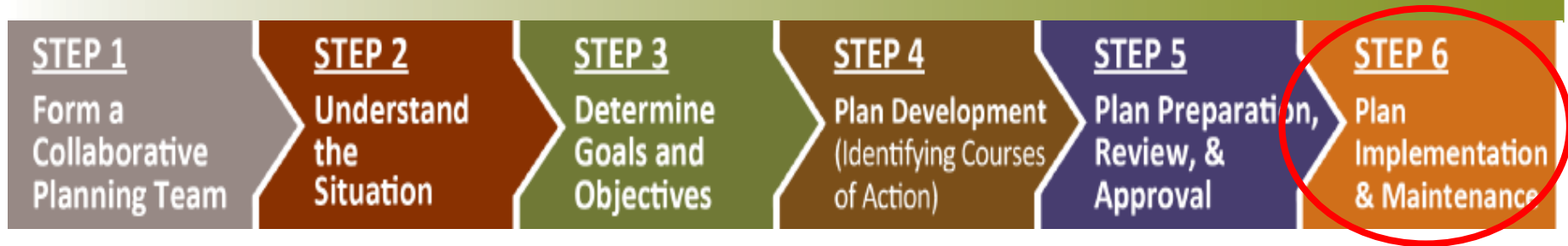
Step 5: Plan Preparation, Review, and Approval



Step 5

- Recommended criteria for a well-designed plan to address cybersecurity include:
 - addressing how the annex connects to State/county/ municipal plans;
 - Identifying chain of command;
 - Including contact information for key staff; and
 - Clearly identifying roles and responsibilities.

Step 6: Plan Implementation and Maintenance



Step 6

- Train stakeholders on the plan to address cybersecurity.
- Conduct emergency drills and exercises related to cybersecurity.
- Conduct after-action reviews of both drills and actual cyber emergencies.
- Identify lessons learned and implement corrective actions.

Agenda

Background on the *Guides* and Integrating Cybersecurity into the Six Step Planning Process

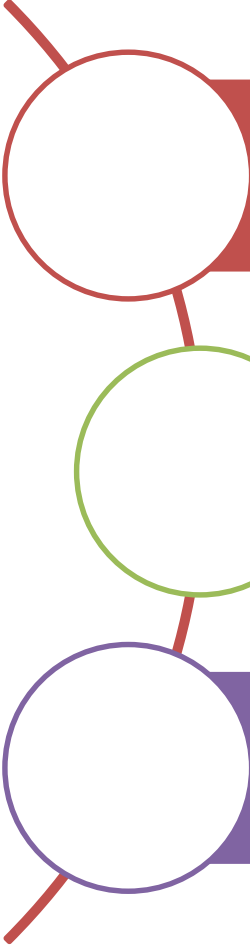
Overview of Cybersecurity

Landscape of IHE Cyber Threats and Trends

DHS Cybersecurity Resources, Programs, and Tools for IHEs

Q&A Session

Overview



Cyber intrusions, data breaches, and attacks at IHEs have increased dramatically over the last decade.

These incidents expose the sensitive personal information of students, faculty, and staff; disrupt critical operations; and impose high financial costs.

DHS offers a variety of resources, programs, and tools to help IHEs establish and maintain secure networks and prevent cyber attacks.

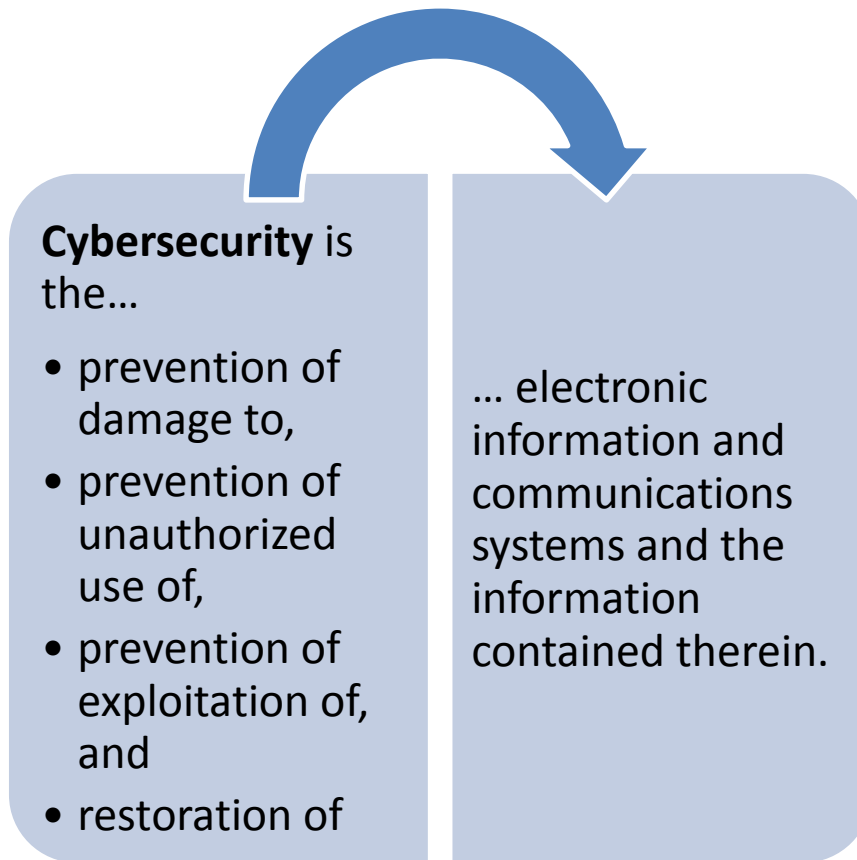
Overview

In coordination with our Federal partners and the private sector, DHS:

- responds to cyber incidents;
- provides technical assistance to owners and operators of critical infrastructure; and
- disseminates notifications regarding current and potential security threats and vulnerabilities.

In addition, the United States Secret Service (USSS) and U.S. Immigration and Customs Enforcement (ICE) investigate Federal cyber crimes, including data breaches, cyber intrusions, and attacks.

Cybersecurity



Cybersecurity is a shared responsibility.

Example Cybersecurity Scenario

The Website of a newspaper is publishing a series of articles discussing the personal financial details of a foreign official.

In response, that foreign country attempts to obtain unauthorized access into the Website to gather the log-in details of the reporter's e-mail to search for information on confidential sources.

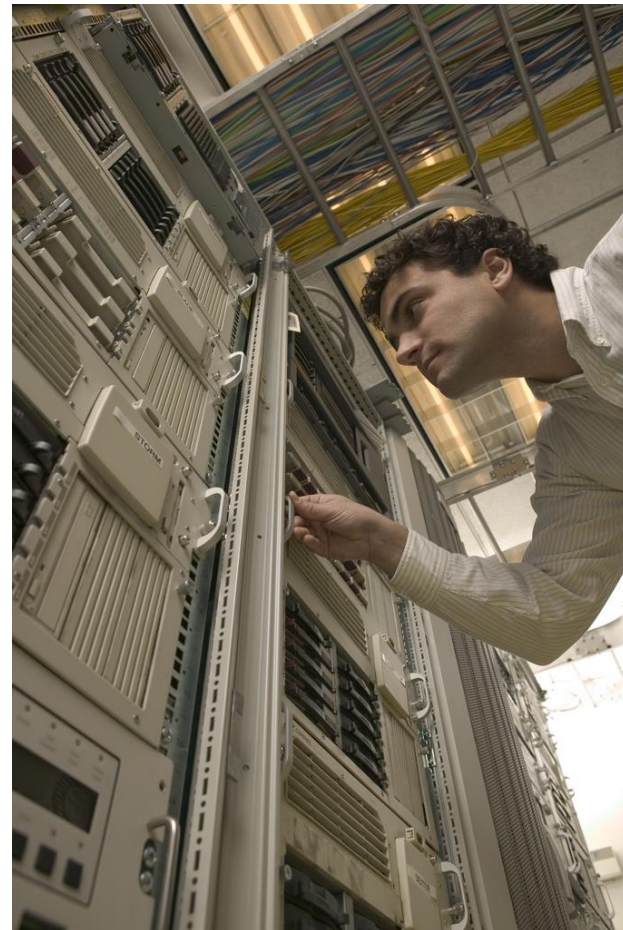
- January 30, 2013: Hackers in China Attacked *The Times* for Last 4 Months

Cyber Systems

Business Systems – Mission essential systems that are used to manage or support common business processes and operations.

Control Systems – Cyber systems used to monitor and control sensitive processes and physical functions

Safety, Security, Support, and Other Specialty Systems – Cyber systems used to manage physical access or for alerting and notification purposes



Cyber Infrastructure

IT systems support business systems, control systems, and security/safety systems.

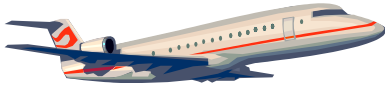


Physical security systems may be connected to the Internet, which can introduce cyber vulnerabilities.



Independently addressing the protection of physical and cyber assets is problematic given the interconnected and interdependent nature of the Nation's critical infrastructure.

Cyber Infrastructure



Agenda

Background on the *Guides* and Integrating Cybersecurity into the Six Step Planning Process

Overview of Cybersecurity

Landscape of IHE Cyber Threats and Trends

DHS Cybersecurity Resources, Programs, and Tools for IHEs

Q&A Session

IHE Cybersecurity In The News

CSU East Bay: 2013 data breach discovered last month

San Jose Mercury News – September 5, 2014

http://www.mercurynews.com/breaking-news/ci_26477689/csu-east-bay-2013-data-breach-discovered-last

U.S. colleges and universities are failing at cybersecurity

eSecurity Planet – August 22, 2014

<http://www.esecurityplanet.com/network-security/u.s.-colleges-and-universities-failing-in-cyber-security.html>

ULM security breach result of e-mail phishing scam

My ArkLaMiss – August 22, 2014

http://www.myarklamiss.com/story/d/story/ulm-security-breach-result-of-e-mail-phishing-scam/15405/Inn-wy3ZaUmo_UGWtMxbVA

E-mail breaches expose over 37,000 people's data at California colleges

eSecurity Planet – June 19, 2014

<http://www.esecurityplanet.com/network-security/e-mail-breaches-expose-over-37000-peoples-data-at-california-colleges.html>

IHE Cyber Trends

Trend	Description	Example
Network and Data Breaches	Outside actors gain unauthorized access to computer networks to destroy/disable systems and/or steal data	In April 2014, the personal information of several thousand students and alumni at a university in Iowa was compromised in a server breach conducted for the purposes of cryptocurrency mining.
Insider Threat	Employees or trusted third parties who intentionally or unintentionally damage/destroy a system and/or steal data	In June 2014, any employee at a major law school mistakenly disseminated personally identifiable information for about 150 students because an incorrect attachment was included on a widely distributed e-mail.

Agenda

Background on the *Guides* and Integrating Cybersecurity into the Six Step Planning Process

Overview of Cybersecurity

Landscape of IHE Cyber Threats and Trends

DHS Cybersecurity Resources, Programs, and Tools for IHEs

Q&A Session

Cybersecurity-Specific Documents

**Presidential Policy Directive (PPD)-21:
Critical Infrastructure Security and Resilience**

National Infrastructure Protection Plan (NIPP)

**Executive Order
13636: Improving
Critical Infrastructure
Cybersecurity**

- **National Institute of Standards and Technology (NIST) Cybersecurity Framework**
- **Critical Infrastructure Cyber Community (C³) Voluntary Program**

DHS Critical Infrastructure Cyber Community Voluntary Program

Critical Infrastructure Cyber Community, or C³ (pronounced “C Cubed”), Voluntary Program

- An innovative public-private partnership to help connect business, Federal government agencies, academia, and State, local, tribal, and territorial (SLTT) government partners to DHS and other Federal government programs and resources that will assist their efforts in managing their cyber risks and using the NIST Cybersecurity Framework.
- For more information on the C³ Voluntary Program, visit <http://www.dhs.gov/ccubedvp> or <http://www.us-cert.gov/ccubedvp>.
- For a list of cybersecurity and cyber risk management resources for the academic community, visit <http://www.us-cert.gov/ccubedvp/getting-started-academia>. Each of the resources is cross walked to Core Functions of the NIST Cybersecurity Framework.

DHS Cybersecurity Assessments, Evaluations and Reviews

Cyber Resilience Review (CRR)

- A no-cost, voluntary, non-technical assessment to evaluate an organization's operational resilience and cybersecurity practices.
- The CRR may be conducted as a downloadable self-assessment or as an on-site assessment facilitated by DHS cybersecurity professionals.
- The review assesses enterprise programs and practices across a range of ten domains, including risk management, incident management, service continuity, and others.
- For more information, visit <http://www.us-cert.gov/ccubedvp/self-service-crr>.

Cybersecurity Evaluation Tool (CSET)

- A self-assessment tool that provides prioritized recommendations and enables users to assess their network and industrial control system security practices against industry and government standards.
- Organizations can also request **On-Site Cybersecurity Consulting**, a facilitated site visit that could include basic security assessments, network architectural review and verification, network scanning using custom tools to identify malicious activity and indicators of compromise, and penetration testing.
- For more information, visit <http://ics-cert.us-cert.gov/assessments>.

DHS Cybersecurity Assessments, Evaluations and Reviews, Continued

Cybersecurity Advisors (CSAs)

- Regionally located DHS personnel who direct coordination, outreach, and regional support to protect cyber components essential to the sustainability, preparedness, and protection of the Nation's critical infrastructure and SLTT governments.
- CSAs offer immediate and sustained assistance to prepare and protect SLTT governments and private entities.
- For more information, email cyberadvisor@hq.dhs.gov.

Protective Security Advisors (PSAs)

- Trained critical infrastructure protection and vulnerability mitigation subject matter experts.
- The PSA program focuses on physical site security and resiliency assessments, planning and engagement, incident management assistance, and vulnerability and consequence information sharing.
- For more information, visit <http://dhs.gov/protective-security-advisors>.

DHS Cybersecurity Information Sharing and Collaboration

Cyber Information Sharing and Collaboration Program (CISCP)

- Enhances cybersecurity collaboration between DHS and critical infrastructure owners and operators, and leverages government and industry subject matter expertise to collaboratively respond to cybersecurity incidents.
- For more information about CISCP, please email ciscp_coordination@hq.dhs.gov.

DHS's Enhanced Cybersecurity Services (ECS) program

- Supports voluntary information-sharing to assist and improve the protection of critical infrastructure systems from unauthorized access, exploitation, or data exfiltration. The program shares cyber threat information with qualified commercial service providers.
- For more information about ECS, please visit <http://www.dhs.gov/enhanced-cybersecurity-services>, or email ECS_Program@HQ.DHS.gov.

DHS Cybersecurity Alerts and Incident Response Assistance

National Cybersecurity & Communications Integration Center (NCCIC)

- A central location where a diverse set of public- and private-sector partners involved in cybersecurity and communications protection coordinate and synchronize their efforts.
- The NCCIC analyzes cybersecurity and communications information; shares timely and actionable information; and coordinates response mitigation and recovery efforts.
- For more information, visit <https://www.dhs.gov/about-national-cybersecurity-communications-integration-center>.

United States Computer Emergency Readiness Team (US-CERT)

- Collaborates with government, private sector, research community, and international entities to monitor cyber trends.
- US-CERT provides access to actionable situational awareness reports; detection information about emerging cyber threats and vulnerabilities, and cybersecurity warning and alert notifications through the **National Cyber Alert System**.
- For more information, visit <http://www.us-cert.gov/>.

DHS Cybersecurity Awareness Campaigns

National Cybersecurity Awareness Month (NCSAM)

- Occurs each October and is designed to engage and educate the public and private sectors to create a safe, secure, and resilient cyber environment.
- Through a series of events and programs across the country, the initiative raises awareness about cybersecurity.
- For more information, visit <http://www.dhs.gov/national-cyber-security-awareness-month>.

Stop.Think.Connect.™ campaign

- A national public awareness campaign aimed at increasing the understanding of cyber threats and empowering the American public to be safer and more secure online.
- The program offers resources and tips for students, young professionals, and educators.
- For more information, visit <http://www.dhs.gov/stopthinkconnect>.

DHS Law Enforcement Resources

United States Secret Service (USSS) and Immigration and Customs Enforcement (ICE)

- DHS law enforcement agencies with jurisdiction over a wide range of Federal crimes that include, but are not limited to, cybercrime, financial crime, and identity theft.
- To report information about possible cyber crime activity, contact your local **USSS** or **ICE** field offices. For more information, visit www.secretservice.gov or www.ice.gov.
- USSS operates the **Electronic Crimes Task Forces (ECTF)**
 - A Network of regional task forces that partner to prevent, detect, mitigate, and investigate various cyber crimes. ECTFs bring together not only Federal, State and local law enforcement, but also prosecutors, private industry, and academia.
 - More than 200 academic institutions are ECTF members.
 - For more information, visit www.secretservice.gov/ectf.shtml.

Additional DHS Resources

Additional tools and resources are also available for academia to use as part of their analytical and protective measures efforts. These include, but are not limited to:

- National Initiative for Cybersecurity Education (NICE) resources;
- National Initiative for Cybersecurity Careers and Studies (NICCS) Portal;
- Cybersecurity Workforce Planning Diagnostic;
- National Cybersecurity Workforce Framework;
- National Centers of Academic Excellence (CAE) resources; and

For more information related to these resources, as well as resources supporting cybersecurity career development and workforce planning, please visit www.us-cert.gov/ccubedvp.

Related Resources & Support


Multi-State Information Sharing and Analysis Center (MS-ISAC)

- The MS-ISAC is the focal point for cyber threat prevention, protection, response and recovery for the nation's State, local, tribal, and territorial (SLTT) governments. The MS-ISAC 24x7 cybersecurity operations center provides real-time network monitoring, early cyber threat warnings and advisories, vulnerability identification and mitigation and incident response.
- For more information, email: info@msisac.org

Research and Education Networking Information Sharing and Analysis Center (REN-ISAC)

- The REN-ISAC aids and promotes cybersecurity operational protection and response within the higher education and research (R&E) communities; within the context of a private community of trusted representatives at member institutions; and in service to the R&E community at-large.
- For more information, visit <http://www.ren-isac.net/>

Related Resources & Support



If you want to receive alerts about **current security issues or vulnerabilities**, visit <http://www.us-cert.gov/ncas/alerts/>.

If you are interested in **conducting a cybersecurity assessment**, visit <http://www.us-cert.gov/ccubedvp/self-service-crr>.

If you are interested in **increasing cyber awareness among your students, faculty, and staff**, visit <http://www.dhs.gov/stopthinkconnect>.

Integrating Cybersecurity into your IHE EOP

The Six Step Planning Process

- Form a Collaborative Planning Team
- Understand the Situation
- Determine Goals & Objectives
- Plan Development
- Plan Preparation, Review, & Approval
- Plan Implementation & Maintenance

Agenda

Background on the Guides & Integrating Cybersecurity into the Six Step Planning Process

Overview of Cybersecurity

Landscape of IHE Cyber Threats and Trends

DHS Cybersecurity Resources, Programs, and Tools for IHEs

Q&A Session

Questions?

Remember to pose your question using the Q&A Chat function on the lower right side of your computer screen.

The REMS TA Center



Phone: (855) 781-7367 (REMS)

Email: info@remstacenter.org

<http://rem.ed.gov>

**Get the
*Guide***

**Join our
Community
of Practice**

**Access
Virtual
Trainings**

**Request an
On-site
Training**